Claims

1. A data playback method for reading protected digital data from a recording medium and playing the read protected digital data, the recording medium having recorded thereon (i) the protected digital data which has been generated by modifying and encrypting original digital data, and (ii) modified restoration-use information which has been generated by modifying restoration-use information that is for use in restoring modified digital data, the data playback method comprising:

a first step of reading the protected digital data from the recording medium, and subjecting the read protected digital data to decryption which corresponds to the encryption, to generate modified digital data;

a second step of subjecting the generated modified digital data to restoration which corresponds to the modification, with use of the restoration-use information, to generate restored digital data;

a third step of playing the generated restored digital data;

a fourth step of reading the modified restoration-use information from the recording medium, and, with use of the read modified restoration-use information, generating the restoration-use information in a format used in processing in the second step; and

a control step of controlling such that the fourth step is executed before the first step.

2. The data playback method of Claim 1, wherein

the generation of the restoration-use information in the fourth step is executed before the playing of the restored digital data, and the first step, the second step, and the third step are executed in parallel during the playing of the restored digital data.

3. The data playback method of Claim 1, wherein

the modification of the restoration-use information is modification that makes the restoration-use information software-tamper-resistant.

4. The data playback method of Claim 1, wherein

the digital data is composed of a plurality of pieces of content, and

execution processing of the restoration-use information differs for each piece of content.

5. The data playback method of any of Claims 1 to 4, wherein

the protected digital data has been generated by encrypting the original digital data and then modifying the encrypted digital data,

in the first step, instead of the decryption, the read protected digital data is subjected to restoration that corresponds to the modification, with use of the restoration-use information, to generate encrypted digital data, and

in the second step, instead of the restoration, the encrypted digital data is subjected to decryption that corresponds to the encryption, to generate the restored digital data.

6. A data playback method for reading protected digital data from a recording medium and playing the read protected digital data, the recording medium having recorded thereon (i) the protected digital data which has been generated by modifying and encrypting original digital data, and (ii) modified restoration-use information which has been generated by modifying restoration-use information that is for use in restoring modified digital data, the data playback method comprising:

a first step of reading the protected digital data from the recording medium, and subjecting the read protected digital data to decryption which corresponds to the encryption, to generate modified digital data;

a second step of subjecting the generated modified digital data to restoration which corresponds to the modification, with use of the restoration-use information, to generate restored digital data;

a third step of playing the generated restored digital data; and

a fourth step of, before the first step, reading the modified restoration-use information from the recording medium, and subjecting the read modified restoration-use information to restoration that corresponds to the modification, to generate unmodified restoration-use information.

7. A data processing apparatus that reads protected digital data from a recording medium and plays the read protected digital data, the recording medium having recorded thereon (i) the protected digital data which has been generated by modifying and encrypting original

digital data, and (ii) modified restoration-use information which has been generated by modifying restoration-use information that is for use in restoring modified digital data, the data processing apparatus comprising:

a reading unit operable to read the protected digital data and the modified restoration-use information from the recording medium;

a decryption unit operable to subject the read protected digital data to decryption corresponding to the encryption, to generate modified digital data;

a restoration unit operable to subject the generated modified digital data to restoration corresponding to the modification, with use of the restoration-use information, to generate restored digital data;

a playback unit operable to play the generated restored digital data;

a generation unit operable to read the modified restoration-use information from the recording medium, and with use of the read modified restoration-use information, generate the restoration-use information in a format used in processing by the restoration unit; and

a control unit operable to control such that the generation of the restoration-use information by the generation unit is executed before the decryption by the decryption unit.

8. The data processing apparatus of Claim 7, wherein

the control unit controls such that the generation of the restoration-use information is executed before playback of the restored digital data, and such that the decryption by the decryption unit, the restoration by the restoration unit and the playback by the playback unit are performed in parallel during playback of the restored digital data.

9. The data processing apparatus of Claim 8, wherein

the modification of the restoration-use information is modification that makes the restoration-use information software-tamper-resistant.

10. The data processing apparatus of Claim 7, wherein

the digital data is composed of a plurality of pieces of content, and

execution processing of the restoration-use information differs for each piece of content.

11. The data processing apparatus of any of Claims 7 to 10, wherein

the protected digital data has been generated by encrypting the original digital data and then modifying the encrypted digital data,

in the decryption unit, instead of the decryption, the read protected digital data is subjected to restoration that corresponds to the modification, with use of the restoration-use information, to generate encrypted digital data, and

in the restoration unit, instead of the restoration, the encrypted digital data is subjected to decryption that corresponds to the encryption, to generate the restored digital data.

12. A data processing apparatus that reads protected digital data from a recording medium and plays the read protected digital data, the recording medium having recorded thereon (i) the protected digital data which has been generated by modifying and encrypting original digital data, and (ii) modified restoration-use information which has been generated by modifying restoration-use information that is for use in restoring modified digital data, the data processing apparatus comprising:

a reading unit operable to read the protected digital data and the modified restoration-use information from the recording medium;

a decryption unit operable to subject the read protected digital data to decryption corresponding to the encryption, to generate modified digital data;

a restoration unit operable to subject the generated modified digital data to restoration corresponding to the modification, with use of the restoration-use information, to generate restored digital data;

a playback unit operable to play the generated restored digital data;

a generation unit operable to read the modified restoration-use information from the recording medium, and subject the modified restoration-use information to restoration corresponding to the modification, to generate unmodified restoration-use information; and

a control unit operable to control such that the generation of the restoration-use information by the generation unit is executed before the decryption by the decryption unit.